

AFFIDAVIT IN SUPPORT SEARCH WARRANT

I, Jamie Frates, a Task Force officer (“TFO”) with the Federal Bureau of Investigation (“FBI”), Kansas City, Missouri, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. As a TFO, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. At all times throughout this affidavit, I use the terms “child sexual abuse material (“CSAM”)” or “child pornography” merely as shorthand to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms “visual depiction,” “minor,” and “sexually explicit conduct” as those terms are defined in 18 U.S.C. § 2256.

2. I am currently employed as a detective with the Kansas City, Missouri Police Department and am serving as a TFO with the FBI. I have been employed with the Kansas City, Missouri Police Department since July 2003, and am currently assigned to the FBI Child Exploitation Task Force, Kansas City, Missouri. Since February 2022, I have been assigned to investigate computer crimes to include violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. These trainings have included instruction related to the laws against sexual abuse of minors, online applications used to entice children to produce sexually explicit material or engage in sexually explicit conduct with adults, and other subjects related to offenses committed against minor children. I have assisted in the investigation of over 30 child pornography cases. During that time, I have had to view thousands of images of child pornography. I have previously applied the federal definition of child pornography used in this affidavit to multiple search warrant applications and a grand jury presentation.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence located at **525 East Armour Boulevard Apt. 111, Kansas City, Missouri 64109** (hereinafter the “**SUBJECT PREMISES**”), which is more particularly described in **Attachment A**, for the items specified in **Attachment B**. I submit there is probable cause to believe that violations of 18 U.S.C. §§2252(a)(2) and (a)(4), that is possession, receipt, and distribution of child pornography, have occurred at the **SUBJECT PREMISES**, and that the evidence, fruits, contraband and instrumentalities of those violations are located at the **SUBJECT PREMISES**.

4. The statements contained in this affidavit are based in part on information provided by law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a TFO with the FBI. Since this affidavit is being submitted for the limited purpose of showing that there is probable cause for the requested warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252, relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually

explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

6. 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving or distributing any visual depiction of minors engaging in sexually explicit conduct in interstate or foreign commerce, by computer or mail. Under 18 U.S.C. § 2252(a)(4), it is also a crime for a person to possess one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce or that were produced using materials that had traveled in interstate or foreign commerce.

PROBABLE CAUSE

7. On November 4, 2022, Affiant was conducting an online investigation on the BitTorrent network for offenders sharing CSAM. Affiant directed his investigative focus to a device at IP address 136.34.111.237 because it was associated with torrents which were identified as having files of investigative interest to CSAM investigations.

8. Using a computer running investigative BitTorrent software, Affiant directly connected to the device at IP address 136.34.111.237, hereinafter referred to as the “**Suspect Device**.” The **Suspect Device** reported that it was using BitTorrent client software AG2584 – Ares 2.5.8.3084 and was sharing three separate torrents. All three of the torrents referenced files that contained CSAM.

9. One torrent had the info hash: ece498c9ee89d817fe72be7ec833916516ef20f4 and referenced 350 files. Between 7:27 AM and 10:55 PM on November 4, 2022, the Affiant successfully completed the download of 24 files from the torrent that the **Suspect Device** was

making available. One of the video files was labeled with a title indicating CSAM related contents. The video was fifty minutes fourteen seconds in length and depicted a nude prepubescent female performing oral sex on an adult male, who then had vaginal sex with her as she is crying.

10. A second torrent had the infohash: 161f0a9499b00cf3e384b8d6d6d06a9a5b0d1327 and referenced 486 files. Between 12:48 PM and 9:38 PM, Affiant successfully completed the download of approximately 56 files from the torrent that the **Suspect Device** was making available. One of the video files was labeled with the title “Kait 5yo”. The video was three minutes thirty-three seconds in length and depicted a naked from the waist down prepubescent female with an adult male who exposes her vagina and buttocks in a lascivious manner. The adult male then inserts his finger and his penis into her exposed vagina.

11. A third torrent had the infohash: 02c1adeaab13784fc1324d887d959c893be17932 and referenced 49 files. Between 12:49 PM and 8:33 PM, Affiant successfully completed the download of approximately 34 files that the **Suspect Device** was making available. One of the video files was labeled with a title indicating CSAM related contents. The video was four minutes nine seconds in length and depicted a pre-teen naked female with an adult male’s erect penis partially inserted into her exposed vagina and anus.

12. Between December 4, 2022, and December 10, 2022, Affiant again directed his investigative focus to the **Suspect Device** because it was associated with additional torrents which were identified as having files of investigative interest to CSAM investigations.

13. On December 4, 2022, a torrent with the info hash: 1bb4ce56d562b41041bba251be23c54894b4ee73 referenced 4,099 files. Between 1:22 AM and 3:11 AM on December 4, 2022, Affiant successfully completed the download of the 2,283 files from the torrent that the **Suspect Device** was making available. Most of the images and videos

visually depicted prepubescent and teenage females engaging in lascivious exhibition of their genitals and engaged in sexually explicit conduct with other adult males, prepubescent and teenage females. One of the video files was fifty-one minutes fifty-seven seconds in length. The video depicted an early teen female sucking on a phallic shaped device, in her underwear. The female then gives oral sex to an adult male who is also giving oral sex to her. The adult male then has vaginal sex with the young female.

14. On December 10, 2022, a torrent with the info hash: f77929f314bc92b11af0eece74e8900f1db6da06 referenced 556 files. Between 5:18 PM and 9:22 PM on October 9, 2022, Affiant successfully completed the download of the 215 files from the torrent that the **Suspect Device** was making available. One of the video files was labeled with a title indicating CSAM related contents. The video was twenty-five seconds in length and depicted a prepubescent female licking an adult male's penis. Another video file depicted an adult male engaging in sexually explicit conduct with an apparent nude female toddler. The video was six minutes thirty-nine seconds in length with the terms "dad", "cumming" and "toddler" in its title.

15. On January 28, 2023, Affiant again directed his investigative focus to the **Suspect Device** because it was associated with an additional torrent which was identified as having files of investigative interest to CSAM investigations.

16. On January 28, 2023, a torrent with the info hash: 0e3615ebad8fdb594653a995f25d588f2d347d62 referenced 5,782 files. Between 5:52 PM and 6:04 PM on January 28, 2023, Affiant successfully completed the download of the 3,280 files from the torrent that the **Suspect Device** was making available. Inside the folder labeled "!!!New 616babypics-mixed & sorted" were images that portrayed prepubescent and early teen females posing in lascivious positions exposing their buttocks and vaginas. One image depicted a naked

infant female with an adult male's penis touching her vagina with apparent semen on the vagina and leg of the infant. Another image depicted an infant with an adult's penis in its mouth.

17. On February 7, 2023, Affiant again directed his investigative focus to the **Suspect Device** because it was associated with an additional torrent which was identified as having files of investigative interest to CSAM investigations.

18. The torrent had the info hash: f77929f314bc92b11af0eece74e8900f1db6da06 and referenced 556 files. Between 5:57 PM on February 7, 2023, and 3:43 PM on February 8, 2023, Affiant successfully completed the download of 33 video files from the torrent that the **Suspect Device** was making available with most depicting CSAM. One of the video files titled "Tara Buttfuck" depicted a prepubescent female being anally sodomized by an adult male. The video is approximately 33 seconds in length.

19. The **Suspect Device** at IP Address 136.34.111.237 was the sole candidate for the downloads referenced above, and as such, each file was downloaded directly from this IP Address.

20. On November 4, 2022, Affiant conducted a query through MAXMIND, a digital mapping company that provides location data for IP addresses. MAXMIND reported that the **Suspect Device** at IP Address 136.34.111.237 was registered to Google Inc. with a possible geo-location address in or near Kansas City, Missouri. On February 10, 2023, an administrative subpoena was served upon Google Inc., for subscriber information.

21. On February 17, 2023, Google's response indicated that the subscriber information for IP address 136.34.111.237 was as follows: Harry Chavez, **525 E. Armour Blvd., Apt. 111, Kansas City, MO 64109-3027**. The primary email address was harrychavezflores1995@gmail.com with an alternate email listed as harry_chavezf@icloud.com. A mobile phone number of 816-517-0133 was listed as a mobile phone number. The account

activation date was on November 1, 2022. The first timestamp for the exact IP address was on November 1, 2022, and the last date stamp was February 16, 2023.

22. Law enforcement database searches revealed Harry Emanuel Chaves Flores, with a date of birth of July 14, 1995, Mexico passport number G41299959, was also associated with the **SUBJECT PREMISES**. Information was also obtained that Chaves Flores was in the U.S. on a Student and Exchange Visa for training at the Westin Crown Center Hotel, Kansas City, Missouri.

23. Contact was made with the Human Resource Department of Westin Crown Center Hotel, where they provided the information as follows: The **SUBJECT PREMISES** is rented by Westin Crown Center for foreign nationals who work for them on Student and Exchange Visas. They also stated there are two individuals that live in that apartment, both being foreign nationals. Information was also provided that the internet and other services are paid for by the tenants and not Westin Hotel. Westin Crown Center Hotel needed a subpoena in order to provide any other information.

24. On February 28, 2023, an administrative subpoena was served upon The Westin at Crown Center, for information on the tenants located at the **SUBJECT PREMISES**.

25. On March 7, 2023, The Westin at Crown Center's response indicated that the tenant information for **SUBJECT PREMISES** was as follows: Harry Chavez, **525 E. Armour Blvd., Apt. 111, Kansas City, MO 64109-3027**, phone numbers 938-194-3522 and 816-517-0133. The other tenant is Nehemiah J. Ferrer with a date of birth January 23, 2000, cell phone 816-517-5993, Philippines Passport #P2372008B, email ferrernehemiah@gmail.com also co-located at **525 E. Armour Blvd., Apt. 111, Kansas City, MO 64109-3027**.

26. On March 30, 2023, the Westin at Crown Center informed Affiant that it believed

Harry Chavez was presently looking for a new residence, indicating that he may be intending to move in the near future.

DEFINITIONS

27. The following definitions apply to this Affidavit and to **Attachment A** to this Affidavit:

a. “Child Erotica,” as used herein, means materials demonstrating a sexual interest in minors, including fantasy narratives, cartoons, and books describing or alluding to sexual activity with minors, sexual aids, children's clothing catalogues, and child modeling images.

b. Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

d. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software,

documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. “Computer software,” as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h.. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

i. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

n. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

o. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

p. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

q. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

r. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

s. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

t. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical

disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS, CELL PHONES, AND CHILD PORNOGRAPHY

28. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

29. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

30. With the advent of digital cameras and cell phones, images can now be transferred directly from a smart phone onto a computer. Images can also be transferred from a computer to a smart phone. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

31. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last

several years. These drives can store thousands of images at very high resolution.

32. A smartphone, or smart phone, is a mobile phone with more advanced computing capability and connectivity than basic feature phones. Early smartphones typically combined the features of a mobile phone with those of another popular consumer device, such as a personal digital assistant (PDA), a media player, a digital camera, or a GPS navigation unit. Modern smartphones include all those features plus the features of a touchscreen computer, including web browsing, Wi-Fi capability, and apps. Frequently, smartphones also include removable storage devices, or SD cards, where users can store data, including picture and video files.

33. Smart phone technology has expanded computer capability in recent years by allowing users to access the Internet via their phone. The smart phone user can search the Internet for specific files, check personal email accounts, log on to social networking sites, communicate with other computer users, compose and edit documents, and store and view movie and picture files.

34. The Internet and its World Wide Web afford collectors of child pornography several different venues and social media platforms for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

35. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as cloud storage, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats.

36. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be

intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data. Even when users delete data, remnants or evidence of that data may still remain within the computer data.

37. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, evidence of child pornography can be found on the user's computer in most cases.

TECHNICAL INFORMATION REGARDING P2P SOFTWARE AND BITTORRENT

38. Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and is often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files. BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the

user will be able to download files from other users on the network and share files from their device with other BitTorrent users.

39. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "info hash", which uniquely identifies the torrent based on the file(s) associated with the torrent file.

40. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

41. Third party software is available to identify the IP address of the P2P computer sending the file and to identify if parts of the file came from one or more IP addresses. Such Software monitors and logs Internet and local network traffic.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

42. Searches and seizures of evidence from cellular phones commonly require agents to download or copy information from the cellular phone to be processed later in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

43. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any application software that may have been used to create the data (whether stored on hard drives or on external media).

SEARCH METHODOLOGY TO BE EMPLOYED

44. The search procedure of electronic data contained in computer hardware, computer software, memory storage devices, and/or cell phones may include the following techniques (the following is a nonexclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, memory storage devices, and/or cell phone to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

**CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN THE
DISTRIBUTION, RECEIPT, OR POSSESSION OF CHILD PORNOGRAPHY OR IN
ATTEMPTS TO COMMIT THOSE CRIMES**

45. As set forth above, probable cause exists to believe that one or more individuals residing at the **SUBJECT PREMISES** has distributed, received or possessed child pornography, or has conspired or attempted to commit these crimes. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

- a. Those who distribute, receive or possess child pornography, or who conspire or attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may

have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who distribute, receive or possess child pornography, or who attempt or conspire to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who distribute, receive or possess child pornography, or who attempt or conspire to commit these crimes often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondences, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. **These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.**

d. Likewise, those who distribute, receive or possess child pornography, or who attempt or conspire to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. **These collections are often maintained for several years and are kept close by, usually on their property including external garages and outbuildings, to enable the collector easier access to view the collection, which is valued highly.**

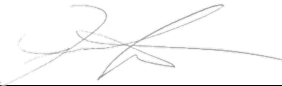
e. Those who distribute, receive or possess child pornography, or who attempt or conspire to commit these crimes also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individual with whom they have been in contact and who share the same interests in child pornography.

f. **Those who distribute, receive or possess child pornography, or who attempt or conspire to commit these crimes prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.**

CONCLUSION

46. Based on the aforementioned factual information, your Affiant respectfully submits that there is probable cause to believe that one or more individuals who reside at the **SUBJECT PREMISES**, more fully described in **Attachment A**, is involved in the distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252 (a)(2) and (a)(4).¹ Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 (a)(2) and (a)(4) (distribution, receipt, and possession of child pornography), is located in the residence described above (the **SUBJECT PREMISES**), and this evidence, listed in **Attachment B** to this affidavit, is contraband or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

47. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the **SUBJECT PREMISES** described in **Attachment A** and seizure and search of the items listed in **Attachment B**.



 Jamie Frates
 Task Force Officer
 Federal Bureau of Investigation

Sworn and subscribed to me by telephone on this 31st day of March 2023.
 at 7:08 p.m.



 HONORABLE JILL A. MORRIS
 United States Magistrate Judge
 Western District of Missouri



¹ In Affiant's experience, multiple occupants of a single residence tend to share access to Internet connections, in particular Wi-Fi connections, thus making it possible that any Internet capable device located within the Subject Premises could have been the Suspect Device in this case.